and the virtual memory when the memory device does not support mutual authentication.

14. (New) The data processing apparatus of claim 13, wherein prior to performing the mutual authentication between the controller and the virtual memory, the controller checks if the memory device supports mutual authentication and, if so, the recording of the data to, or reproduction of the data from, the memory device is conditioned upon the establishment of the mutual authentication between the controller and the memory device.

15. (New) The data processing apparatus of claim 13 wherein the mutual authentication is performed between the controller and the virtual memory by applying an authenticating key stored in the virtual memory and an enabling key block distribution authenticating key, wherein the enabling key block distribution authenticating key is previously enciphered by an enabling key block comprising enciphering data for enciphering renewal keys on paths of a hierarchical key tree structure comprising a variety of keys disposed in correspondence with roots, nodes, and leaves of the key tree structure on paths ranging from roots to leaves of the key tree structure, and wherein the data processing apparatus is associated with one of the leaves of the key tree structure, and wherein said enciphering data further comprises upper-rank keys to be enciphered by lower-rank keys.

16. (New) The data processing apparatus according to claim 15, wherein the data processing apparatus is properly licensed if the data processing apparatus is enabled to decode the enabling key block and wherein the data processing apparatus is devoid of proper licensing if unable to decode the enabling key block.

17. (New) The data processing apparatus according to claim 15 wherein the enabling key block distribution authenticating key enciphered by the enabling key block is subject to a version controlling process by way of executing a process for renewing individual versions on the controller.

18. (New) The data processing apparatus according to claim 13 further comprising a memory for storing an enciphered leaf key, the enciphered leaf key produced by enciphering a leaf key by a storage key that is associated with the data processing apparatus, and wherein the leaf key is a part of a hierarchical key tree structure comprising a variety of keys disposed in correspondence with roots, nodes, and leaves of the key tree structure on paths ranging from roots to leaves of the key tree structure, and wherein the leaf key is associated with the data processing apparatus.

19. (New) The data processing apparatus according to claim 13 further comprising a memory for storing a device key block comprising an assemblage of ciphered keys further comprising mutually different individually enciphered node keys of a hierarchical key tree structure comprising a variety of keys disposed in correspondence with roots, nodes, and leaves of the key tree structure on paths ranging from roots to leaves of the key tree structure, and wherein one of the leaves is associated with the data processing apparatus.

20. (New) A method for use in a device for recording data to, or reproducing data from, a memory device, the method comprising the steps of:

(a) executing a mutual authentication process with a virtual memory device when the memory device does not support the mutual authentication process; and

(b) if the mutual authentication between the device and the virtual memory is successful, executing the recording of the data to, or the reproduction of the data from, the memory device.

21. (New) The method of claim 20 further comprising the steps of:

(c) prior to step (a), identifying whether the memory device supports the mutual authentication process; and

(d) if the memory device supports the mutual authentication process, skipping step (a) and executing the mutual authentication process with the memory device for the purpose of recording data to, or reproducing data from, the memory device.

22. (New) The method of claim 20 wherein the mutual authentication process is executed between the device and the virtual memory by applying an authenticating key stored in the virtual memory and an enabling key block distribution authenticating key, wherein the enabling key block distribution authenticating key is previously enciphered by an enabling key block comprising enciphering data for enciphering renewal keys on paths of a hierarchical key tree structure comprising a variety of keys disposed in correspondence with roots, nodes, and leaves of the key tree structure on paths ranging from roots to leaves of the key tree structure, and wherein the device is associated with one of the leaves of the key tree structure, and wherein said enciphering data further comprises upper-rank keys to be enciphered by lower-rank keys.

23. (New) A license system for use in a data processing system, the license system comprising:

a means for providing an enabling key block distribution authenticating key, wherein the enabling key block distribution authenticating key is previously enciphered by an enabling key block comprising enciphering data for enciphering renewal keys on paths of a hierarchical key tree structure comprising a variety of keys disposed in correspondence with roots, nodes, and leaves of the key tree structure on paths ranging from roots to leaves of the key tree structure, and wherein at least one of the leaves of the key tree structure is associated with a device, and wherein said enciphering data further comprises upper-rank keys to be enciphered by lower-rank keys;

a means for executing a process for reproducing data from, or recording data to, a memory device solely based on condition that a mutual authentication is actually effectuated between the device and the memory device even when the memory device is devoid of function to execute mutual authentication with the device; and

wherein the device is properly licensed if the device is enabled to decode the enabling key block and wherein the device is devoid of proper licensing if unable to decode the enabling key block.

24. (New) A computer-readable medium for storing computer-executable software code for the execution of the recording of data to, or the reproduction of data from, a memory device, said code comprising:

code for executing a mutual authentication process with a virtual memory device when the memory device does not support the mutual authentication process; and

code for executing the recording of the data to, or the reproduction of the data from, the memory device if the if the mutual authentication between the device and the virtual memory is successful.